CLAIMS

1. A method for controlling transmission of messages in a data communication network, each message is associated with a message source, comprising:

providing a store and forward relay, the relay associated with a plurality of recipients receiving messages;

the relay receiving a message intended for a recipient associated with the e-mail network;

the relay applying a first filtering policy to the message;

the relay delaying the delivery of the message in response to at least one predetermined result of applying said first filtering policy;

the relay applying a second filtering policy to the message after a delay period; and

the relay delivering the message in response to at least one predetermined result of applying said second filtering policy.

2. The method of Claim 1, wherein said first and second filter policies are different policies.
3. The method of Claim 1, wherein said relay is an email relay applying e-mail filtering policies to received messages.
4. The method of Claim 1, wherein said relay is acting as an intermediate node for a store and forward email protocol.
5. The method of Claim 1, wherein said relay is acting as a final node for a store and forward email protocol.
6. The method of Claim 1, wherein said relay applying a second filter policy is by reference to a time based event.

7. The method of Claim 1, wherein said second filter policy is provided by updating at least a portion of the data associated with a previous version of the second filter policy by reference to data received from a third party server.
8. The method of Claim 7, wherein the updating of said second filter policy includes updating code employed by an ant virus program module.
9. The method of Claim 7, wherein the updating of said second filter policy is by periodic data downloads from one or more servers.
10. The method of Claim 7, wherein the updating of said second filter policy is by automatic update messages from a third party.
11. The method of Claim 7, wherein the updating of said second filter policy is by a manual request from an administrator.
12. The method of Claim 1, wherein said applying the second policy is initiated at a time based on at least one condition selected from the group consisting of time since first delay, time since first delay as a function of the current time, the fact that the second policy has been updated since the message was delayed, current time, current date, and current day of the week.
13. The method of Claim 1, wherein the message is associated with an SMTP transmission protocol.
14. The method of Claim 1, wherein the relay is the final destination server of the message and is further configured to manage delivery of the message to the recipient.
15. The method of Claim 1, wherein the relay comprises components which are distributed across several physical computers but act logically as a single system.
16. The method of Claim 1, wherein the public network is the Internet.

17. The method of Claim 1, wherein said at least one predetermined action comprises adding said message data to the SPAM database.

18. The method of claim 1, wherein said applying a filtering policy comprises:

identifying a comparison for evaluating by reference to the message;

identifying at least one evaluation associated with the comparison;

for each evaluation associated with the comparison:

extracting data from the message in accordance with parameters associated with the identified evaluation;

executing the evaluation for the extracted data by comparing the extracted data to data from the SPAM database;

determining a new comparison score based on the executed evaluation; and

determining that the message is SPAM if the comparison score is beyond a threshold.

19. The method of claim 18, wherein the threshold is a threshold range.

20. The method of Claim 18, wherein the relay combines the evaluations using a scoring formula with weighing associated with evaluations and employs resultant score to determine the action to take.

21. The method of Claim 18, wherein the relay combines the condition using a statistical formula to determine the action to take.

22. The method of Claim 18, wherein the relay combines the condition using a probabilistic formula to determine the action to take.

23. The method of Claim 18, wherein the relay combines the condition using Bayesian statistical analysis.

24. The method of Claim 18, wherein said at least one evaluation comprises comparing the sender address of the message to a sender address of records in the SPAM database.

25. The method of Claim 18, wherein said at least one evaluation refers to at least one recipient of the message.

26. The method of Claim 18, wherein said at least one evaluation refers to the header of the message.

27. The method of Claim 18, wherein said at least one evaluation refers to the subject field of the message header.

28. The method of Claim 18, wherein said at least one evaluation refers to the textual content of the message body including the presence of keywords.

29. The method of Claim 18, wherein said at least one evaluation refers to the overall size of the message.

30. The method of Claim 18, wherein said at least one evaluation refers to the message body format, including the presence of an HTML format.

31. The method of Claim 18, wherein said at least one evaluation refers to the HTML construct if the HTML format is present.

32. The method of Claim 18, wherein said at least one evaluation refers to a URL that may be present in the message body and attachments.

33. The method of Claim 18, wherein said at least one evaluation refers to the number of attachments.

34. The method of Claim 18, wherein said at least one evaluation refers to the size of attachments.

35. The method of Claim 18, wherein said at least one evaluation refers to the type of attachments.

36. The method of Claim 18, wherein said at least one evaluation refers to the name of attachments.

37. The method of Claim 18, wherein said at least one evaluation refers to the content of attachments.

38. The method of Claim 18, wherein said at least one evaluation refers to the validity of digital signatures in the message and attachments.

39. The method of Claim 18, wherein said at least one evaluation refers to the fact that the message follows a standards format.

40. The method of Claim 18, wherein said at least one evaluation refers to a hash of at least a portion of the message and comparison of the hash against a database of hash values.

41. The method of Claim 18, wherein said at least one evaluation refers to the presence of malicious code in the message and attachments.

42. The method of Claim 18, wherein said at least one evaluation refers to time indicators associated with the message.

43. The method of Claim 18, wherein said at least one evaluation refers to the fact that the message is processed after delaying delivery of the message.

44. The method of Claim 18, wherein said at least one evaluation refers to the time period since delivery delay was initiated for the message.

45. The method of Claim 18, wherein said at least one evaluation refers to the IP and domain of the sender.

46. The method of Claim 18, wherein said at least one evaluation refers to the transport protocol session, including envelope sender and recipient.

47. The method of Claim 1, wherein the relay is further configured to take an action in response to applying said first policy, said action is selected from the group consisting of deliver normally, return to sender, copy to a recipient, send a blind copy to a recipient, forward to a recipient, delete the message, delay delivery and move to an area for review by an administrator, delay delivery and move to an area for future review by an external user, delay delivery and move to an area for future review by a recipient, save a copy of the message, and move the message to a delayed delivery area.

48. The method of Claim 47, wherein evaluations and corresponding actions are different at least between two recipients.

49. The method of Claim 47, wherein the relay is further configured to modify attributes of the message, including subject, headers, body, and attachments.

50. The method of Claim 47, wherein the modifying is on copies of the message when applying the policy results in different modification for different recipients.

51. The method of Claim 47, wherein the modifying of the message consists of removing malicious code in the message.

52. The method of Claim 47, wherein the association between evaluations and actions is configurable by an administrator.

53. The method of Claim 47, wherein the association between evaluations and actions is configured by the recipient of the message.